Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for providing public key infrastructure security in a computer network comprising:

a user terminal coupled to the computer network;

a user transaction data record assigned to the user, wherein the user transaction data record includes a raw state, an unleased state, an assigned state and a leased state, and a data element indicating a present operational state of the user transaction data record ~~three or more predetermined states for the user transaction data record,~~ including one of the raw state, the unleased state, the assigned state and the leased state, wherein only a predetermined type of commands are allowed to be executed on the user transaction data record for each ~~predetermined~~ operational state;

a private key, and a public key assigned to a user for ~~authenticating~~ encrypting and decrypting the user transaction data record~~, when the user registers with the system using the user terminal~~;

a database remote from the user terminal for securely storing the encrypted user transaction data record, and the private key and the public key ~~in the user transaction data record~~; and

a cryptographic device remote from the user terminal and coupled to the computer network including a computer executable code ~~for signing~~ to encrypt and decrypt the data in the user transaction data record utilizing the stored private key and the public key in the database, and ~~for executing~~ to execute one or more of the commands that are allowed for [[a]] the present state of the user transaction data record.

2. (Canceled)

3. (Original) The system of claim 1, wherein the private key is encrypted when it is stored in the database.

4. (Previously Presented) The system of claim 2, wherein a respective security device transaction data related to a user is loaded into the cryptographic device when the user requests a service.

5. (Previously Presented) The system of claim 1, wherein the cryptographic device is configured to authenticate the identity of the user and verify that the identified user is authorized to assume a role and perform a corresponding operation.

6. (Original) The system of claim 5, wherein the assumed role is a security officer role to initiate a key management function.

7. (Original) The system of claim 5, wherein the assumed role is an administrator role to manage a user access control database.

8. (Original) The system of claim 5, wherein the assumed role is a provider role to withdraw from a user account.

9. (Original) The system of claim 5, wherein the assumed role is a user role to operate on a value bearing item.

10. (Original) The system of claim 5, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

11. (Original) The system of claim 5, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

12. (Original) The system of claim 5, wherein the cryptographic device stores information about a number of last transactions in a respective internal register.

13. (Original) The system of claim 12, wherein the database stores a table including the respective information about a last transaction, a verification module to compare the information saved in the device with the information saved in the database.

14. (Original) The system of claim 1,further comprising a digital certificate stored in the database and assigned to a user when the user registers with the system.

15. (Previously Presented) The system of claim 1, wherein the cryptographic device is configured for digitally signing a certificate.

16. (Previously Presented) The system of claim 1, w erein the cryptographic device is configured for encrypting data.

17. (Previously Presented) The system of claim 1, w erein the cryptographic device is configured for decrypting data.

18. (Original) The system of claim 1, wherein the database includes a user profile for the user.

19. (Original) The system of claim 18, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period.

20. (Original) The system of claim 5, wherein the cryptographic device is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

21. (Original) The system of claim 5, wherein the cryptographic device stores information about a number of last transactions in an internal register and compares the information saved in the register with the information saved in a memory before loading a new transaction data.

22. (Currently Amended) A method for providing public key infrastructure security in a computer network comprising the steps of:

assigning a private key and a public key to a user for authenticating a user transaction data record, wherein the user transaction data record includes a raw state, an unleased state, an assigned state and a leased state, and a data element indicating ~~three or more predetermined states~~ a present operational state of the user transaction data record including one of the raw state, the unleased state, the assigned state and the leased state ~~for the user transaction data record~~, wherein only a predetermined type of commands are allowed to be executed on the user transaction data record for each ~~predetermined~~ state;

storing the private key, the public key and the user transaction data record in a database remote from the user terminal;

~~signing~~ encrypting the data in the user transaction data record assigned to the user utilizing the stored private key and the public key in the database; and

controlling the user transaction data record to execute one or more of the commands that are allowed for [[a]] the present state of the user transaction data record.

23. (Original) The method of claim 22, further comprising the step of storing a digital certificate and assigning the stored digital certificate to a user when the user registers with the system.

24. (Canceled)

25. (Previously Presented) The method of claim 24, further comprising the step of loading the user transaction data related to a user into the cryptographic device when the user requests to operate on a value bearing item.

26. (Original) The method of claim 25, further comprising the step of verifying that the requesting user is authorized to assume a role and to perform a corresponding operation.

27. (Original) The method of claim 26, wherein the assumed role is an administrator role to manage a user access control.

28. (Original) The method of claim 26, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

29. (Original) The method of claim 26, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

30. (Original) The method of claim 26, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.

31. (Previously Presented) The method of claim 25, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database;

comparing the information saved in the respective device with the respective information saved in the database; and

loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

32. (Previously Presented) The method of claim 22, further comprising digitally signing a certificate.

33. (Previously Presented) The method of claim 22, further comprising encrypting data.

34. (Previously Presented) The method of claim 22, further comprising decrypting data.

35. (Original) The method of claim 22, further comprising the step of storing a user profile for a plurality of users.

36. (Original) The method of claim 35, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period

37. (Original) The method of claim 22, wherein the cryptographic function is one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature,SHA-1, and Pseudo-random number generation algorithms.

38 (New) A system for providing public key infrastructure security in a computer network comprising:

a user terminal coupled to the computer network;

a user transaction data record assigned to the user, wherein the user transaction data record includes a data element indicating three or more predetermined operational states for the user transaction data record, wherein only a predetermined type of commands are allowed to be executed on the user transaction data record for each predetermined operational state;

a private key, and a public key assigned to a user for authenticating the user transaction data record;

a database remote from the user terminal for securely storing the user transaction data record, and the private key and the public key in the user transaction data record; and

a cryptographic device remote from the user terminal and coupled to the computer network including a computer executable code for signing the data in the user transaction data record utilizing the stored private key in the database, and for executing one or more of the commands that are allowed for a present state of the user transaction data record, wherein the cryptographic device includes three or more states, and wherein only a predetermined type of commands are executed by the cryptographic device for each state.